Amendments to the Claims

Claim 1 (original): A security container that secures a document component by encapsulating, within the security container, the document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component.

Claim 2 (original): The security container according to Claim 1, wherein the security container secures a portion of a higher-level document.

Claim 3 (original): The security container according to Claim 2, wherein the higher-level document has more than one portion secured by security containers.

Claim 4 (original): A method of securing document content using security containers, comprising the step of encapsulating, within a security container, a document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component.

Claim 5 (original): The method according to Claim 4, wherein the key distribution information further comprises an identification of one or more users and/or processes that are authorized to access the document component.

Claim 6 (original): The method according to Claim 5, wherein the key distribution information

further comprises a symmetric key that encrypted both the document component and the conditional logic that are encapsulated within the security container, wherein the symmetric key is stored in an encrypted form for decryption by the authorized users and/or processes.

Claim 7 (original): The method according to Claim 6, wherein the encrypted form of the symmetric key comprises a separate version of the key for each distinct user, process, group of users, or group of processes, wherein the separate version has been encrypted with a public key associated with the corresponding distinct user, process, group of users, or group of processes.

Claim 8 (original): The method according to Claim 5, wherein the authorized users and/or the authorized processes are specified individually or as groups.

Claim 9 (original): The method according to Claim 4, wherein the conditional logic further controls access to the document component.

Claim 10 (original): The method according to Claim 9, wherein the key distribution information further controls access to the conditional logic.

Claim 11 (original): The method according to Claim 4, wherein the document component and the conditional logic are encrypted before encapsulation within the security container.

Claim 12 (original): The method according to Claim 4, wherein the security container is encoded

in structured document format.

Claim 13 (original): The method according to Claim 12, wherein the structured document format is Extensible Markup Language ("XML") format.

Claim 14 (original): The method according to Claim 5, wherein the identification of the one or more users and/or processes comprises an identification of at least one group, the group having as members one or more of the users and/or processes.

Claim 15 (original): The method according to Claim 14, wherein the members are determined dynamically, upon receiving a request to access to the document component.

Claim 16 (original): The method according to Claim 15, wherein the dynamic determination further comprises accessing a repository where the members of the group are identified.

Claim 17 (original): The method according to Claim 4, further comprising the steps of:

receiving, from a requester, a request to access the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and rejecting the request when the programmatically determining step has a negative result.

Claim 18 (original): The method according to Claim 17, wherein the conditional logic evaluates at least one of: an identity of the requester; a device used by the requester; a context of the requester; a zone of an application used by the requester; a user profile of the requester; and a target destination of the request.

Claim 19 (original): A computer program product for securing document content using security containers, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

computer-readable program code means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

computer-readable program code means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the computer-readable program code means for programmatically determining yields a positive result, and for rejecting the request when operation of the computer-readable program code means for programmatically determining yields a negative result.

Claim 20 (original): A system for securing document content using security containers, comprising:

a security container that encapsulates a document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component;

means for receiving, from a requester, a request to access the document component;

means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the means for programmatically determining yields a positive result, and for rejecting the request when operation of the means for programmatically determining yields a negative result.

Claim 21 (original): The system according to Claim 20, wherein the security container is embedded within a document.

Claim 22 (original): The system according to Claim 20, wherein the security container encapsulates the document component on a system clipboard.

Claim 23 (original): The system according to Claim 20, wherein the security container is placed on a user interface.

Claim 24 (original): The system according to Claim 20, wherein the security container encapsulates the document component for exchange using interprocess communications.

Claim 25 (original): The system according to Claim 20, wherein the security container encapsulates the document component for exchange using a messaging system.

Claim 26 (original): The system according to Claim 20, further comprising means for copying the document component to a target destination, wherein the means for copying copies the entire security container in order to copy the document component.

Claim 27 (original): A method of securing document content using security containers, comprising steps of:

receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component;

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and for rejecting the request when the programmatically determining step has a negative result; and

charging a fee for carrying out one of more of the receiving, programmatically determining, and programmatically evaluating steps.

Claim 28 (original): A method of securing document content using security containers, comprising steps of:

receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component;

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and for rejecting the request when the programmatically determining step has a negative result; and

charging a fee to the requester when the programmatically evaluating step determines that the request can be granted.

Claim 29 (new): The method according to Claim 5, further comprising the steps of:

sending the security container to one or more recipients; and

upon receipt at each of the recipients, using the conditional logic to determine whether that recipient can access the document component encapsulated within the security container.

Claim 30 (new): The method according to Claim 5, further comprising the steps of:

receiving, at a recipient, the security container; and

using the conditional logic to determine whether the recipient can access the document component encapsulated within the security container.

Claim 31 (new): The method according to Claim 5, further comprising the steps of:

receiving, at a plurality of recipients, the security container; and

using the conditional logic, at one or more of the recipients, to determine whether that recipient can access the document component encapsulated within the security container.

Claim 32 (new): The method according to Claim 4, wherein the security container encapsulates the document component for transfer to a plurality of members of a group, and wherein each member of the group to which the transfer is made uses the conditional logic for determining whether that member is authorized to access the document component.